Invertible Matrices over Finite Additively Idempotent Semirings

Andreas Kendziorra
Claude Shannon Institute
University College Dublin

Stefan E. Schmidt
Institut für Algebra
Technische Universität Dresden

Jens Zumbrägel
Claude Shannon Institute
University College Dublin

Abstract

We investigate invertible matrices over finite additively idempotent semirings. The main result provides a criterion for the invertibility of such matrices. We also give a construction of the inverse matrix and a formula for the number of invertible matrices.

Keywords: Matrix inversion, Semirings, Lattices.

2010 Mathematics Subject Classification: 15A09, 15B99, 16Y60, 06B10.

1 Introduction

Monico, Maze, and Rosenthal generalized in [10] the Diffie-Hellman protocol, which is used in public-key cryptography, by using arbitrary semigroup actions instead of the group exponentiation. Some of the proposed actions involve matrices over proper finite simple semirings with zero. Monico showed in [11] that these semirings are additively idempotent and Zumbrägel presented in [16] a characterization of these semirings, which can be formulated by residuated mappings of finite lattices. When matrices are used for cryptographic purposes, the principal questions arise how to easily decide whether a matrix is invertible and, if so, how to compute the inverse matrix. For matrices over fields the answers are well-known: A matrix over a field is invertible iff its determinant is nonzero, and the inverse of an invertible matrix can be computed, e.g., with the help of Gauss-Jordan elimination. A similar useful criterion for invertible matrices over arbitrary semirings is not known in general. There are results for invertible matrices over boolean algebras [9, 12, 14]. Furthermore, there exist generalizations to matrices over certain ordered algebraic structures [2], and there are results for matrices over Brouwerian lattices [15] and distributive lattices [5]. Also for matrices over certain commutative semirings some results are known [4, 13].

This work has been supported by Science Foundation Ireland under grant no. 08/IN.1/I1950.

In this paper we present a criterion for invertible matrices over finite additively idempotent semirings with zero and one. As an important consequence, for a finite additively idempotent base semiring with irreducible additive semigroup we get that a matrix is invertible iff it is a generalized permutation matrix. Besides the criterion, we present a construction for the inverse of an invertible matrix and a formula for the number of invertible matrices of a given size over a given semiring. For these results we represent a finite additively idempotent semiring with zero and one as a semiring of residuated mappings of a finite lattice. The invertibility criterion is then based on a description of automorphisms of lattices. The results cover the case of invertible matrices over proper finite simple semirings with zero, which are used in [10].

2 Matrices over additively idempotent semirings

Definition 2.1. Let R be a nonempty set and $+$ and $\cdot$ two binary operations on R. Then $(R, +, \cdot)$ is called a *semiring* if $(R, +)$ is a commutative semigroup, $(R, \cdot)$ is a semigroup and the distributive laws $r \cdot (s + t) = r \cdot s + r \cdot t$ and $(r + s) \cdot t = r \cdot t + s \cdot t$ for all $r, s, t \in R$ hold. If a neutral element 0 of the semigroup $(R, +)$ exists and it satisfies $0 \cdot x = x \cdot 0 = 0$ for all $x \in R$, then it is called a *zero*. If a neutral element 1 of the semigroup $(R, \cdot)$ exists, then it is called a *one*. A semiring is called a *proper* semiring if it is not a ring, i.e., $(R, +)$ is not a group.

For invertible matrices over semirings we clearly have just to consider semirings with zero and one.

A *lattice* $\mathbf{L} = (L, \leqslant)$ is an ordered set where for every two elements $x, y \in L$ the supremum $x \vee y$ and the infimum $x \wedge y$ in L exists. $\mathbf{L}$ is called *complete* if for every subset $X \subseteq L$ the supremum $\bigvee X$ and the infimum $\bigwedge X$ in L exists. A complete lattice has a greatest element $1_{\mathbf{L}}$ and a least element $0_{\mathbf{L}}$.

There exists an equivalent definition of lattices as algebras: A *lattice* is an algebra $(L, \vee, \wedge)$, where L is a nonempty set, and $\vee$ and $\wedge$ are binary, associative, commutative operations on L, which fulfill the absorption laws $x \vee (x \wedge y) = x$ and $x \wedge (x \vee y) = x$ for every $x, y \in L$. That these two definitions are equivalent can be found in [6].

If $\mathbf{L}$ and $\mathbf{K}$ are complete lattices and a mapping $f : L \to K$ fulfills $f(\bigvee X) = \bigvee f(X)$ for every subset $X \subseteq L$, then f is called *residuated* (residuated mappings are usually defined more generally for arbitrary ordered sets, but for complete lattices this definition is sufficient; see [3]). If $\mathbf{L}$ and $\mathbf{K}$ are finite then $f : L \to K$ is residuated iff $f(x \vee y) = f(x) \vee f(y)$ for every $x, y \in L$ and $f(0_{\mathbf{L}}) = 0_{\mathbf{K}}$. By $\mathrm{Res}(\mathbf{L})$ we denote the set of all residuated mappings from $\mathbf{L}$ to $\mathbf{L}$. The structure $(\mathrm{Res}(\mathbf{L}), \vee, \circ)$, where $\vee$ denotes the pointwise supremum and $\circ$ the composition of two mappings, is a semiring. Further the mapping $\mathbf{0} : L \to L,\ x \mapsto 0_{\mathbf{L}}$, is a zero and id_L a one of this semiring. More information about lattices can be found in [1, 6] and about residuated mappings in [3].

If $(R, +)$ is a commutative idempotent semigroup, then $(R, \leqslant)$ with $x \leqslant y :\Leftrightarrow x + y = y$ is a semilattice with the supremum operation $\vee = +$. If $(R, +)$ is further finite and has a neutral element then $(R, \leqslant)$ is even a lattice (see [1]). Hence, if $(R, +, \cdot)$ is a finite additively idempotent semiring with zero, then $(R, \leqslant)$ is a lattice. The next proposition shows that one can embed such a semiring into a semiring of residuated mappings if it has additionally a one.

Proposition 2.2. *Let $(R,+,\cdot)$ be a finite additively idempotent semiring with zero and one, $\mathbf{R} := (R,\leqslant)$ and*

$$T : R \to \mathrm{Res}(\mathbf{R}) , \quad r \mapsto T_r \quad \textit{with} \quad T_r : x \mapsto rx .$$

Then $(R,+,\cdot)$ is isomorphic to the subsemiring $(T(R),\vee,\circ)$ of $(\mathrm{Res}(\mathbf{R}),\vee,\circ)$.

Proof. Clearly, $T_r \in \mathrm{Res}(\mathbf{R})$ for every $r \in R$ and T is a semiring homomorphism between $(R,+,\cdot)$ and $(\mathrm{Res}(\mathbf{R}),\vee,\circ)$. Since $(R,+,\cdot)$ has a one 1, we have that $T_r = T_s$ implies $r = T_r(1) = T_s(1) = s$ for all $r,s \in R$, i.e., T is injective. Hence, $(R,+,\cdot)$ is isomorphic to the subsemiring $(T(R),\vee,\circ)$ of $(\mathrm{Res}(\mathbf{R}),\vee,\circ)$. □

Next we present the characterization of proper finite simple semirings with zero by Zumbrägel [16], which was in combination with [10] the motivation for this work.

Definition 2.3. Let $\mathbf{A} = (A,F)$ be an algebra. A *congruence* on $\mathbf{A}$ is an equivalence relation θ on A with the following property: For every $n \in \mathbb{N}$ and every n-ary mapping $f \in F$ and elements $a_i, b_i \in A$ with $a_i \theta b_i$ for $1 \leqslant i \leqslant n$, it holds that $f(a_1,...,a_n)\theta f(b_1,...,b_n)$.

For a homomorphism $f : \mathbf{A} \to \mathbf{B}$ of some algebras $\mathbf{A},\mathbf{B}$ of the same type the *kernel* $\ker(f) := \{(a,a') \in A \times A \mid f(a) = f(a')\}$ of f is a congruence on $\mathbf{A}$. Also the *equality relation* $\Delta_A := \{(a,a) \mid a \in A\}$ and the *complete relation* $\nabla_A := A \times A$ are congruences on $\mathbf{A}$. Congruences are one of our main tools to derive our results. For a wider background on congruences and universal algebra see [7].

Definition 2.4. A semiring $(R,+,\cdot)$ is called *simple* if its only congruences are Δ_R and ∇_R.

For a complete lattice $\mathbf{L} = (L,\leqslant)$ and $a,b \in L$ define a mapping $e_{a,b} \in \mathrm{Res}(\mathbf{L})$ by

$$e_{a,b} : L \to L , \quad x \mapsto \begin{cases} 0_{\mathbf{L}} & \text{if } x \leqslant a, \\ b & \text{otherwise.} \end{cases}$$

The main result from [16] can be stated as follows:

Theorem 2.5. *Let $\mathbf{L}$ be a finite lattice and $(R,\vee,\circ)$ a subsemiring of $(\mathrm{Res}(\mathbf{L}),\vee,\circ)$ such that $e_{a,b} \in R$ for every $a,b \in L$. Then $(R,\vee,\circ)$ is a proper finite simple semiring with zero. Conversely, every proper finite simple semiring $(S,+,\cdot)$ with $|S| > 2$ and a zero is isomorphic to such a semiring.*

For two monoids $\mathbf{M}$ and $\mathbf{N}$ we denote by $\mathrm{Hom}(\mathbf{M},\mathbf{N})$ the set of all monoid homomorphism from $\mathbf{M}$ to $\mathbf{N}$ and by $\mathrm{End}(\mathbf{M})$ the set of all endomorphisms of $\mathbf{M}$. Let I be a finite index set and $\mathbf{M}_i$ commutative monoids for every $i \in I$. It is easy to see that the mapping

$$\Omega : \bigtimes_{(i,j)\in I\times I} \mathrm{Hom}(\mathbf{M}_j,\mathbf{M}_i) \to \mathrm{End}\Big(\bigtimes_{i\in I} \mathbf{M}_i\Big) , \quad (f_{i,j}) \mapsto \Big(\sum_{j\in I} f_{i,j}\Big)_{i\in I}$$

with

$$\Big(\sum_{j\in I} f_{i,j}\Big)_{i\in I}\big((m_j)_{j\in I}\big) = \Big(\sum_{j\in I} f_{i,j}(m_j)\Big)_{i\in I}$$

for every $(m_j)_{j\in I} \in \bigtimes_{j\in I} \mathbf{M}_j$ is an isomorphism between the semirings

$$\Big(\bigtimes_{(i,j)\in I\times I} \mathrm{Hom}(\mathbf{M}_j, \mathbf{M}_i), +, \cdot\Big) \quad \text{and} \quad \Big(\mathrm{End}\big(\bigtimes_{i\in I} \mathbf{M}_i\big), +, \circ\Big),$$

where $+$ denotes in each case the pointwise sum, $\circ$ on $\mathrm{End}(\bigtimes_{i\in I} \mathbf{M}_i)$ the composition, and $\cdot$ is defined on $\bigtimes_{(i,j)\in I\times I} \mathrm{Hom}(\mathbf{M}_j, \mathbf{M}_i)$ by $(f_{i,j}) \cdot (g_{i,j}) =: (h_{i,j})$ with $h_{i,j} = \sum_{k\in I} f_{i,k} \circ g_{k,j}$. In particular, it holds that

$$\big(\mathrm{Mat}_{I\times I}(\mathrm{End}(\mathbf{M})), +, \cdot\big) := \Big(\bigtimes_{(i,j)\in I\times I} \mathrm{End}(\mathbf{M}), +, \cdot\Big) \cong \big(\mathrm{End}(\mathbf{M}^I), +, \circ\big),$$

where $\mathbf{M}^I := \bigtimes_{i\in I} \mathbf{M}$.

If $\mathbf{L}$ and $\mathbf{K}$ are finite lattices and $f : L \to K$ is a mapping, then f is residuated iff f is a monoid homomorphism between the monoids $(L, \vee, 0_{\mathbf{L}})$ and $(K, \vee, 0_{\mathbf{K}})$. Hence, we get

$$\big(\mathrm{Mat}_{I\times I}(\mathrm{Res}(\mathbf{L})), +, \cdot\big) \cong \big(\mathrm{Res}(\mathbf{L}^I), \vee, \circ\big).$$

Therefore, a matrix $M = (m_{i,j}) \in \mathrm{Mat}_{I\times I}(\mathrm{Res}(\mathbf{L}))$ is invertible iff the corresponding residuated mapping

$$\varphi_M := \big(\bigvee_{j\in I} m_{i,j}\big)_{i\in I} \in \mathrm{Res}(\mathbf{L}^I)$$

is invertible, which is equivalent to φ_M being bijective.

A mapping $f : P \to Q$ between ordered sets $(P, \leqslant)$ and $(Q, \leqslant)$ is an *(order) isomorphism* if f is surjective and it fulfills $x \leqslant y \Leftrightarrow f(x) \leqslant f(y)$ for all $x, y \in P$. Note that an order isomorphism is automatically injective. An order isomorphism from $(P, \leqslant)$ to $(P, \leqslant)$ is called *(order) automorphism*. Note in the following that the concepts of isomorphisms and automorphisms of lattices as ordered sets and as algebras are equivalent (see [6]).

Lemma 2.6. *Let* $\mathbf{L}$ *be a complete lattice and* $f \in \mathrm{Res}(\mathbf{L})$*. Then* f *is an automorphism of* $\mathbf{L}$ *iff* f *is bijective.*

Proof. Let f be bijective. For $x, y \in L$, the equivalence $x \leqslant y \Leftrightarrow y = x \vee y \Leftrightarrow f(y) = f(x \vee y) = f(x) \vee f(y) \Leftrightarrow f(x) \leqslant f(y)$ holds, i.e., f is an automorphism. The other direction is clear. □

Corollary 2.7. *Let* $\mathbf{L}$ *be a finite lattice,* I *a finite index set, and* $M = (m_{i,j}) \in \mathrm{Mat}_{I\times I}(\mathrm{Res}(\mathbf{L}))$*. Then* M *is invertible iff the corresponding mapping* $\varphi_M \in \mathrm{Res}(\mathbf{L}^I)$ *is an automorphism of* $\mathbf{L}^I$*.*

Hence, we aim to give a characterization for when a mapping of the direct product $\mathbf{L}^I$ is an automorphism of $\mathbf{L}^I$. If $\mathbf{L}$ is a direct product $\bigtimes_{t\in T} \mathbf{L}_t$ of irreducible lattices $\mathbf{L}_t$, $t \in T$, for a finite index set T, our task is then to determine when a mapping of the direct product $(\bigtimes_{t\in T} \mathbf{L}_t)^I$ is an automorphism. Consequently, it suffices to find a criterion for mappings of direct products of irreducible lattices. We present such a criterion (Theorem 4.1) and we translate it so that we can answer the question when a matrix in $\mathrm{Mat}_{I\times I}(\mathrm{Res}(\mathbf{L}))$ is invertible (Corollary 4.2). In Section 4.4 we explain how our results apply to subsemirings of $(\mathrm{Res}(\mathbf{L}), \vee, \circ)$, so that, by Proposition 2.2, they can be applied to every finite additively idempotent semiring with zero and one.

3 Direct decompositions

In this section we investigate maximal direct decompositions of lattices, on which our criterion for matrix invertibility will crucially depend.

An algebra $\mathbf{A} = (A, F)$ is called *trivial* if $|A| = 1$, otherwise it is called *nontrivial*. We call an algebra $\mathbf{A}$ *irreducible* if it is nontrivial and not isomorphic to a direct product of two nontrivial algebras. Analogously, an ordered set $\mathbf{P} = (P, \leqslant)$ is called *trivial* if $|P| = 1$, otherwise it is called *nontrivial*. We also call an ordered set $\mathbf{P}$ *irreducible* if it is nontrivial and not isomorphic to a direct product of two nontrivial ordered sets. Clearly, the direct product of lattices as ordered sets is the same as the direct product of lattices as algebras. Consequently, a lattice is irreducible as an ordered set iff it is irreducible as an algebra.

Definition 3.1. A *subdirect decomposition* of an algebra $\mathbf{A}$ is a family $(\Theta_t)_{t\in T}$ of congruences of $\mathbf{A}$ with

$$\bigcap_{t\in T} \Theta_t = \Delta_A \,.$$

We call a subdirect decomposition $(\Theta_t)_{t\in T}$ of $\mathbf{A}$ a *direct decomposition* of $\mathbf{A}$ if the mapping

$$\iota : A \to \bigtimes_{t\in T} A/\Theta_t, \quad a \mapsto \big([a]\Theta_t\big)_{t\in T}$$

is surjective. Moreover, we call a direct decomposition $(\Theta_t)_{t\in T}$ of $\mathbf{A}$ *maximal* if $\Theta_t \neq \nabla_A$ for every $t \in T$ and if for every direct decomposition $(\Theta_s)_{s\in S}$ of $\mathbf{A}$ with $\Theta_s \neq \nabla_A$ for every $s \in S$ the inequality $|S| \leqslant |T|$ holds.

The mapping ι is for every algebra $\mathbf{A}$ and every subdirect decomposition $(\Theta_t)_{t\in T}$ of $\mathbf{A}$ an injective homomorphism. Therefore, $\mathbf{A}$ is isomorphic to $\iota(\mathbf{A})$. If ι is even surjective, then $\mathbf{A}$ is isomorphic to the direct product $\times_{t\in T} \mathbf{A}/\Theta_t$. If Θ_t is non-total for a $t \in T$, then the factor $\mathbf{A}/\Theta_t$ is nontrivial.

Let $\mathbf{A}_i$, $i \in I$, be some nontrivial algebras of the same type and let $\mathbf{A} := \times_{i\in I} \mathbf{A}_i$. For an element $a \in A$, we denote by a_i the i-th coordinate of a. Define the congruence $\Phi_i := \{(a, b) \in A \times A \mid a_i = b_i\}$ for every $i \in I$. Then $(\Phi_i)_{i\in I}$ is clearly a direct decomposition of $\mathbf{A}$ and Φ_i is non-total for every $i \in I$. Thus for a maximal direct decomposition $(\Theta_t)_{t\in T}$ of $\mathbf{A}$, the inequality $|T| \geqslant |I|$ holds.

The next proposition is stated in [8].

Proposition 3.2. *The representation of a connected ordered set as the direct product of irreducible ordered sets is unique up to pairwise isomorphism of the factors.*

Since a lattice is a connected ordered set, we get the following.

Corollary 3.3. *Let S and T be index sets, $\mathbf{L}_t$ an irreducible lattice for every $t \in T$, $\mathbf{L} := \times_{t\in T} \mathbf{L}_t$, and $(\Theta_s)_{s\in S}$ a maximal direct decomposition of $\mathbf{L}$. Then there exists a bijection $\sigma : S \to T$ with $\mathbf{L}/\Theta_s \cong \mathbf{L}_{\sigma(s)}$.*

For this reason, we may assume that if $\mathbf{L}$ is the direct product of the irreducible lattices $\mathbf{L}_t$, $t \in T$, then a maximal direct decomposition of $\mathbf{L}$ is of the form $(\Theta_t)_{t\in T}$ with $\mathbf{L}/\Theta_t \cong \mathbf{L}_t$ for all $t \in T$.

In [6, Chapter 1.3, Theorem 13] the following result is proven.

Theorem 3.4. *Let* $\mathbf{L}$ *and* $\mathbf{K}$ *be lattices, let* Θ_L *be a congruence on* $\mathbf{L}$*, and let* Θ_K *be a congruence on* $\mathbf{K}$*. Define the relation* $\Theta_L \times \Theta_K$ *on* $\mathbf{L} \times \mathbf{K}$ *by*

$$(a,b)(\Theta_L \times \Theta_K)(c,d) \quad \textit{iff} \quad a\Theta_L c \ \textit{ and } \ b\Theta_K d\,.$$

Then $\Theta_L \times \Theta_K$ *is a congruence on* $\mathbf{L} \times \mathbf{K}$*. Conversely, every congruence on* $\mathbf{L} \times \mathbf{K}$ *is of this form.*

Note that '$\Theta_L \times \Theta_K$' is a slight abuse of notation, since it is not identical to the Cartesian product of the two sets Θ_L and Θ_K.

It further holds that

$$[a]\Theta_L \times [b]\Theta_K = \{(c,d) \in L \times K \mid a\Theta_L c \text{ and } b\Theta_K d\} = [(a,b)](\Theta_L \times \Theta_K) \quad (1)$$

and so

$$\mathbf{L}/\Theta_L \times \mathbf{K}/\Theta_K = (\mathbf{L} \times \mathbf{K})/(\Theta_L \times \Theta_K)\,. \quad (2)$$

The following result is a strengthening of Corollary 3.3.

Lemma 3.5. *Let* T *be a finite index set,* $\mathbf{L}_t$ *an irreducible lattice for every* $t \in T$*,* $\mathbf{L} := \bigtimes_{t\in T} \mathbf{L}_t$*, and* $(\Theta_t)_{t\in T}$ *a maximal direct decomposition of* $\mathbf{L}$*. Then there exists a permutation* σ *of* T *with* $\mathbf{L}_t \cong \mathbf{L}_{\sigma(t)}$ *and*

$$(x_s)_{s\in T}\Theta_{\sigma(t)}(y_s)_{s\in T} \quad \Leftrightarrow \quad x_t = y_t$$

for all $(x_s)_{s\in T}, (y_s)_{s\in T} \in L$ *and* $t \in T$*.*

Proof. By Corollary 3.3, we may assume that $\mathbf{L}/\Theta_t \cong \mathbf{L}_t$ holds for all $t \in T$. We fix $t_0 \in T$ and define $\mathbf{L}' := \bigtimes_{t\in T\setminus\{t_0\}} \mathbf{L}_t$. Thus, $\mathbf{L} = \mathbf{L}_{t_0} \times \mathbf{L}'$. By Theorem 3.4, there exist for every $t \in T$ congruences $\Theta_t^{t_0} \in \mathrm{Con}(\mathbf{L}_{t_0})$, $\Theta_t' \in \mathrm{Con}(\mathbf{L}')$ with $\Theta_t = \Theta_t^{t_0} \times \Theta_t'$. We will show that $(\Theta_t^{t_0})_{t\in T}$ is a direct decomposition of $\mathbf{L}_{t_0}$. Let $(x,x') \in \bigcap_{t\in T} \Theta_t^{t_0}$. We have to show that $x = x'$ holds. Let $\bar{y} \in L'$. Thus, $(\bar{y},\bar{y}) \in \bigcap_{t\in T} \Theta_t'$ and consequently $((x,\bar{y}),(x',\bar{y})) \in \bigcap_{t\in T} \Theta_t = \Delta_L$. So, we have $(x,\bar{y}) = (x',\bar{y})$ and therefore $x = x'$. Hence, $(\Theta_t^{t_0})_{t\in T}$ is a subdirect decomposition of $\mathbf{L}_{t_0}$. Now let $x_t \in \mathbf{L}_{t_0}$ for every $t \in T$. We will show that there exists an element $z \in \mathbf{L}_{t_0}$ with $[z]\Theta_t^{t_0} = [x_t]\Theta_t^{t_0}$ for every $t \in T$. Choose an element $(y_t)_{t\in T\setminus\{t_0\}} \in \mathbf{L}'$. For every $s \in T$ we will regard $(x_s, (y_t)_{t\in T\setminus\{t_0\}}) \in L$ as the element in L, where the t_0-th coordinate is x_s. Since $(\Theta_t)_{t\in T}$ is a direct decomposition of $\mathbf{L}$, there exists an element $(\hat{x}_t)_{t\in T} \in L$ with $[(\hat{x}_t)_{t\in T}]\Theta_s = [(x_s, (y_t)_{t\in T\setminus\{t_0\}})]\Theta_s$ for every $s \in T$. By Equation (1), for every $s \in T$,

$$\begin{aligned}[\hat{x}_{t_0}]\Theta_s^{t_0} \times [(\hat{x}_t)_{t\in T\setminus\{t_0\}}]\Theta_s' = [(\hat{x}_t)_{t\in T}]\Theta_s &= [(x_s, (y_t)_{t\in T\setminus\{t_0\}})]\Theta_s \\ &= [x_s]\Theta_s^{t_0} \times [(y_t)_{t\in T\setminus\{t_0\}}]\Theta_s'\end{aligned}$$

holds and it follows that $[\hat{x}_{t_0}]\Theta_s^{t_0} = [x_s]\Theta_s^{t_0}$. Hence, $\hat{x}_{t_0}$ is the desired element z and it follows that $(\Theta_t^{t_0})_{t\in T}$ is a direct decomposition of $\mathbf{L}_{t_0}$. Consequently, $\mathbf{L}_{t_0} \cong \bigtimes_{t\in T}(\mathbf{L}_{t_0}/\Theta_t^{t_0})$ and since $\mathbf{L}_{t_0}$ is irreducible, there exists a unique $t_1 \in T$ with $\mathbf{L}_{t_0} \cong \mathbf{L}_{t_0}/\Theta_{t_1}^{t_0}$. Thus, $\Theta_{t_1}^{t_0} = \Delta_{L_{t_0}}$. By this and Equation (2), it follows that

$$\mathbf{L}_{t_0} \times \mathbf{L}'/\Theta_{t_1}' \cong \mathbf{L}_{t_0}/\Theta_{t_1}^{t_0} \times \mathbf{L}'/\Theta_{t_1}' = (\mathbf{L}_{t_0} \times \mathbf{L}')/(\Theta_{t_1}^{t_0} \times \Theta_{t_1}') = \mathbf{L}/\Theta_{t_1} \cong \mathbf{L}_{t_1}\,.$$

Since $\mathbf{L}_{t_1}$ is irreducible and $\mathbf{L}_{t_0}$ nontrivial, we have $\mathbf{L}_{t_0} \cong \mathbf{L}_{t_1}$ and $|\mathbf{L}'/\Theta_{t_1}'| = 1$. Hence, $\Theta_{t_1}' = \nabla_{L'}$. We derive $(x_t)_{t\in T}\Theta_{t_1}(y_t)_{t\in T} \Leftrightarrow x_{t_0} = y_{t_0}$ for all $(x_t)_{t\in T}, (y_t)_{t\in T} \in L$.

We have shown that there exists a mapping $\sigma : T \to T$ with $\mathbf{L}_t \cong \mathbf{L}_{\sigma(t)}$ and $(x_s)_{s\in T}\Theta_{\sigma(t)}(y_s)_{s\in T} \Leftrightarrow x_t = y_t$ for all $(x_s)_{s\in T}, (y_s)_{s\in T} \in L$. Indeed, with the notation above we have $t_1 = \sigma(t_0)$. It remains to show that σ is injective. Let $t_2, t_3 \in T$ with $\sigma(t_2) = \sigma(t_3)$. There follows the equivalence $x_{t_2} = y_{t_2} \Leftrightarrow (x_t)_{t\in T}\Theta_{\sigma(t_2)}(y_t)_{t\in T} \Leftrightarrow (x_t)_{t\in T}\Theta_{\sigma(t_3)}(y_t)_{t\in T} \Leftrightarrow x_{t_3} = y_{t_3}$ for all $(x_t)_{t\in T}$, $(y_t)_{t\in T} \in L$ and we find that $t_2 = t_3$. □

4 Invertible matrices

4.1 A criterion

The following theorem states a criterion for a mapping of a direct product of irreducible lattices to be an automorphism. It is basically a consequence of Lemma 3.5. We will see the corresponding result for matrices in Corollary 4.2.

Theorem 4.1. *Let T be a finite index set, $\mathbf{L}_t$ an irreducible lattice for every $t \in T$, $\mathbf{L} := \times_{t\in T} \mathbf{L}_t$, and $\varphi : L \to L$ a mapping. Then $\varphi \in \mathrm{Aut}(\mathbf{L})$ iff there exists a permutation σ of T and isomorphisms $\varphi_t : L_t \to L_{\sigma^{-1}(t)}$ for every $t \in T$ such that*

$$\varphi = (\varphi_{\sigma(t)} \circ \pi_{\sigma(t)})_{t\in T} ,$$

where π_t is the t-th projection, i.e., $\varphi((x_t)_{t\in T}) = (\varphi_{\sigma(t)}(x_{\sigma(t)}))_{t\in T}$ for all $(x_t)_{t\in T} \in L$.

Proof. Let $\varphi \in \mathrm{Aut}(\mathbf{L})$, $\varphi^t := \pi_t \circ \varphi$ for every $t \in T$, and $\Theta_t := \ker(\varphi^t)$ for every $t \in T$. We will show that $(\Theta_t)_{t\in T}$ is a maximal direct decomposition of $\mathbf{L}$. We have

$$\begin{aligned}(x, y) \in \bigcap_{t\in T} \Theta_t \;&\Leftrightarrow\; \forall t \in T : (x, y) \in \Theta_t \\ &\Leftrightarrow\; \forall t \in T : \varphi^t(x) = \varphi^t(y) \;\Leftrightarrow\; \varphi(x) = \varphi(y) \;\Leftrightarrow\; x = y\end{aligned}$$

for all $x, y \in L$, i.e., $\bigcap_{t\in T} \Theta_t = \Delta_L$. Therefore, $(\Theta_t)_{t\in T}$ is a subdirect decomposition of $\mathbf{L}$. Let $y^t \in L$ for every $t \in T$. We will show that there exists a $z \in L$ with $[z]\Theta_t = [y^t]\Theta_t$ for every $t \in T$. Let $x_t := \varphi^t(y^t)$ for every $t \in T$, let $x := (x_t)_{t\in T}$, and let $z := \varphi^{-1}(x)$. It follows that $\varphi^t(z) = x_t = \varphi^t(y^t)$ and therefore that $z\Theta_t y^t$ for every $t \in T$. Hence, $[z]\Theta_t = [y^t]\Theta_t$ for every $t \in T$ and $(\Theta_t)_{t\in T}$ is consequently a direct decomposition. Since φ is bijective, $\Theta_t \neq \nabla_L$ holds for every $t \in T$. Because a maximal direct decomposition of $\mathbf{L}$ has exactly $|T|$ elements by Corollary 3.3, $(\Theta_t)_{t\in T}$ is a maximal direct decomposition.

By Lemma 3.5, there exists a permutation σ of T with $\mathbf{L}_t \cong \mathbf{L}_{\sigma(t)}$ and $x\Theta_t y \Leftrightarrow x_{\sigma(t)} = y_{\sigma(t)}$ for every $t \in T$ and $x, y \in L$. It follows that $\varphi^t(x) = \varphi^t(y) \Leftrightarrow x\Theta_t y \Leftrightarrow x_{\sigma(t)} = y_{\sigma(t)}$, i.e., $\varphi^t(x)$ depends only on $x_{\sigma(t)}$ for every $t \in T$. With $\varphi_{\sigma(t)} := \varphi^t \circ \epsilon_{\sigma(t)}$, where $\epsilon_s : L_s \to L$ is the s-th canonical injection, it follows that the given criterion is necessary.

The sufficiency of the criterion is trivial. □

Let T, I be finite index sets, $\mathbf{L}_t$ an irreducible finite lattice for every $t \in T$, and $\mathbf{L} := \times_{t\in T} \mathbf{L}_t$. Then $\mathbf{L}^I = \times_{(t,i)\in T\times I} \mathbf{L}_{t,i}$, where $\mathbf{L}_{t,i} = \mathbf{L}_t$ for every $(t, i) \in T \times I$. With this notation we derive in the following the corresponding result for invertible matrices. For a matrix $A \in \mathrm{Mat}_{I\times I}(\mathrm{Res}(\mathbf{L}))$, we will denote the i-th row by A_i and we will regard A_i as mapping from L^I to L.

Corollary 4.2. *Let T, I be finite index sets, $\mathbf{L}_t$ an irreducible finite lattice for every $t \in T$, $\mathbf{L} := \bigtimes_{t\in T} \mathbf{L}_t$, and $A = (a_{i,j}) \in \mathrm{Mat}_{I\times I}(\mathrm{Res}(\mathbf{L}))$. Then A is invertible iff there exists a permutation σ of $T \times I$ and an isomorphism $\varphi_{t,i} : L_{t,i} \to L_{\sigma^{-1}(t,i)}$ for every $(t, i) \in T \times I$ such that*

$$\pi_t \circ A_i = \varphi_{\sigma(t,i)} \circ \pi_{\sigma(t,i)} \,,$$

where π_t is the projection from $\mathbf{L}$ to $\mathbf{L}_t$ and $\pi_{t,i}$ the projection from $\mathbf{L}^I$ to $\mathbf{L}_{t,i}$.

If A is invertible, then

$$\varphi_A = \big(\varphi_{\sigma(t,i)} \circ \pi_{\sigma(t,i)}\big)_{(t,i)\in T\times I}$$

is the corresponding mapping of A in $\mathrm{Res}(\mathbf{L}^I)$ and $a_{i,j}$ is of the form $a_{i,j} = (\hat{\varphi}_{i,j,t})_{t\in T}$ with

$$\hat{\varphi}_{i,j,t} = \begin{cases} \varphi_{\sigma(t,i)} & \text{if } \exists s \in T : \sigma(t,i) = (s,j), \\ \bar{0}_{\mathbf{L}_t} & \text{otherwise,} \end{cases}$$

where $\bar{0}_{\mathbf{L}_t}$ is the mapping that maps constantly to $0_{\mathbf{L}_t}$.

In the special case where $\mathbf{L}$ is irreducible, we need not to consider the index set T, since it has just one element. Then the equation in Corollary 4.2 is of the form $A_i = \varphi_{\sigma(i)} \circ \pi_{\sigma(i)}$ for every $i \in I$, i.e., $a_{i,\sigma(i)}$ is the only nonzero entry in the i-th row and $a_{i,\sigma(i)} = \varphi_{\sigma(i)}$ holds. We call a matrix a *generalized permutation matrix* (or *monomial matrix*) if each row and each column has exactly one nonzero entry and this nonzero entry is invertible.

Corollary 4.3. *Let $\mathbf{L}$ be a finite irreducible lattice, I a finite index set, and $A \in \mathrm{Mat}_{I\times I}(\mathrm{Res}(\mathbf{L}))$. Then A is invertible iff A is a generalized permutation matrix.*

4.2 Number of invertible matrices

As another consequence of Theorem 4.1 we find the following.

Corollary 4.4. *Let T be a finite index set, $\mathbf{L}_t$, $t \in T$, pairwise distinct irreducible lattices, $e_t \in \mathbb{N}$ for every $t \in T$, and $\mathbf{L} := \bigtimes_{t\in T} \mathbf{L}_t^{e_t}$. Then*

$$|\operatorname{Aut}(\mathbf{L})| = \prod_{t\in T} e_t! \cdot |\operatorname{Aut}(\mathbf{L}_t)|^{e_t} \,.$$

In particular, for a finite index set I we have

$$|\operatorname{Aut}(\mathbf{L}^I)| = \prod_{t\in T} (e_t \cdot |I|)! \cdot |\operatorname{Aut}(\mathbf{L}_t)|^{e_t\cdot|I|} \,,$$

which is exactly the number of invertible matrices in $\mathrm{Mat}_{I\times I}(\mathrm{Res}(\mathbf{L}))$.

4.3 The inverse matrix

The next proposition provides a construction for the inverse matrix of an invertible matrix.

Proposition 4.5. *Let T, I be finite index sets, $\mathbf{L}_t$ an irreducible finite lattice for every $t \in T$, $\mathbf{L} := \times_{t\in T} \mathbf{L}_t$, let $A = (a_{i,j}) \in \mathrm{Mat}_{I\times I}(\mathrm{Res}(\mathbf{L}))$ be invertible, and σ and $\varphi_{t,i}$ for every $(t,i) \in T \times I$ as in Corollary 4.2. Then for the inverse matrix $B = (b_{i,j})$ of A, the entry $b_{i,j}$ for $i, j \in I$ is of the form $b_{i,j} = (\check{\varphi}_{i,j,t})_{t\in T}$ with*

$$\check{\varphi}_{i,j,t} = \begin{cases} \varphi_{t,i}^{-1} & \text{if } \exists s \in T : \sigma^{-1}(t,i) = (s,j), \\ \bar{0}_{\mathbf{L}_t} & \text{otherwise.} \end{cases}$$

Proof. As stated before, $\varphi_A = (\varphi_{\sigma(t,i)} \circ \pi_{\sigma(t,i)})_{(t,i)\in T\times I}$ is the corresponding mapping to A in $\mathrm{Res}(\mathbf{L}^I)$. The inverse of φ_A, i.e., the corresponding mapping to the matrix B, is the mapping $\varphi_B = \varphi_A^{-1} = (\varphi_{t,i}^{-1} \circ \pi_{\sigma^{-1}(t,i)})_{(t,i)\in T\times I}$. It follows that $b_{i,j}$ is of the form $b_{i,j} = (\check{\varphi}_{i,j,t})_{t\in T}$ with $\check{\varphi}_{i,j,t}$ as given in the proposition. □

4.4 Invertible matrices over subsemirings of $\mathrm{Res}(\mathbf{L})$

Lemma 4.6. *Let $\mathbf{L}$ be a finite lattice, $(R, \vee, \circ)$ a subsemiring of $(\mathrm{Res}(\mathbf{L}), \vee, \circ)$, and $\varphi \in R$ such that φ is invertible in $(\mathrm{Res}(\mathbf{L}), \circ)$. Then $\varphi^{-1} \in R$.*

Proof. Since φ is invertible and $\mathbf{L}$ is finite, we find that $\varphi^{-1} \in \langle\varphi\rangle \subseteq R$, where $\langle\varphi\rangle$ is the span of φ with respect to $\circ$. □

If $(R, \vee, \circ)$ is a subsemiring of $(\mathrm{Res}(\mathbf{L}), \vee, \circ)$, then $(\mathrm{Mat}_{I\times I}(R), +, \cdot)$ is also a subsemiring of $(\mathrm{Mat}_{I\times I}(\mathrm{Res}(\mathbf{L})), +, \cdot)$. The next corollary states the corresponding result.

Corollary 4.7. *Let $\mathbf{L}$ be a finite lattice, $(R, \vee, \circ)$ a subsemiring of $(\mathrm{Res}(\mathbf{L}), \vee, \circ)$, I a finite index set, and $A \in \mathrm{Mat}_{I\times I}(R)$ such that A is invertible in $\mathrm{Mat}_{I\times I}(\mathrm{Res}(\mathbf{L}))$. Then $A^{-1} \in \mathrm{Mat}_{I\times I}(R)$.*

This means that for matrices over a subsemiring of $\mathrm{Res}(L)$ one can also apply Corollary 4.2 to decide whether a matrix is invertible and Proposition 4.5 to construct the inverse of an invertible matrix. Consequently, one can do this for every finite additively idempotent semiring with zero and one by Proposition 2.2. In particular, these results apply to every proper finite simple semiring with zero by Theorem 2.5.

4.5 Remarks

In the following let $(R, +, \cdot)$ be a finite additively idempotent semiring with zero and one. To apply Corollary 4.2 and Proposition 4.5 for matrices over R, it is necessary to represent the semiring as a semiring of residuated mappings of a finite lattice $\mathbf{L}$. Additionally, it is required to know the representation of the lattice as a direct product $\mathbf{L} = \times_{t\in T} \mathbf{L}_t$ of irreducible lattices $\mathbf{L}_t$ and to represent every residuated mapping (semiring element) as a mapping of $\times_{t\in T} \mathbf{L}_t$. For example, one can represent $(R, +, \cdot)$ as the subsemiring $(T(R), \vee, \circ)$ of $(\mathrm{Res}(\mathbf{R}), \vee, \circ)$, where $\mathbf{R} = (R, \leqslant)$ (see Proposition 2.2). Also in this case, one has to represent $\mathbf{R}$ as a direct product $\mathbf{R} = \times_{t\in T} \mathbf{R}_t$ of irreducible lattices $\mathbf{R}_t$, and one has to represent every mapping in $T(R)$ as a mapping of $\times_{t\in T} \mathbf{R}_t$.

If the lattice $\mathbf{L}$ is irreducible, then we know by Corollary 4.3 that a matrix is invertible iff it is a generalized permutation matrix. In this case, determining whether a matrix is invertible as well as inverting is very easy. In particular,

if the lattice $\mathbf{R}$ is irreducible, then a matrix is invertible iff it is a generalized permutation matrix. Furthermore, the lattice $\mathbf{R}$ is irreducible iff the semigroup $(R, +)$ is irreducible. Hence, we get the following corollary.

Corollary 4.8. *Let $(R, +)$ be irreducible and $A \in \mathrm{Mat}_{I\times I}(R)$. Then A is invertible iff A is a generalized permutation matrix.*

If $\mathbf{L}$ is given without the representation as a direct product of irreducible lattices, then it may actually be involved to find such a representation. In particular, it can be hard to find such a representation for $\mathbf{R}$. In the cryptographic application described in [10] it may be sensible for the involved parties of the protocol (Alice and Bob) to agree in the setup phase on a random finite simple semiring by choosing randomly a finite lattice $\mathbf{K}$ and taking $(\mathrm{Res}(\mathbf{K}), \vee, \circ)$ (or a certain subsemiring $(R, \vee, \circ)$ with $e_{a,b} \in R$ for all $a, b \in K$) as the semiring. If one picks randomly a finite lattice, then the chosen lattice is likely to be irreducible, and thus determining whether a matrix over this semiring is invertible and computing the inverse of an invertible matrix gets again very easy, since all invertible matrices are in this case generalized permutation matrices.

In order to prevent that deciding whether a matrix is invertible and computing the inverse become easy problems, a possible approach is that the parties agree on several irreducible lattices and publish the direct product of these lattices, without showing the representation of this lattice as a direct product.

References

[1] G. Birkhoff, *Lattice Theory*, Third edition, American Mathematical Society, Providence, R.I., 1967

[2] T. S. Blyth, *Matrices Over Ordered Algebraic Structures*, J. London Math. Soc., Vol. 39, No. 1, 1964, pp. 427–432

[3] T. S. Blyth, M. F. Janowitz, *Residuation Theory*, Pergamon Press, Oxford, 1972

[4] D. Dolžan, P. Oblak, *Invertible and Nilpotent Matrices Over Antirings*, Linear Algebra Appl., Vol. 430, 2009, pp. 271–278

[5] Y. Give'on, *Lattice Matrices*, Information and Control, Vol. 7, No. 4, 1964, pp. 477–484

[6] G. Grätzer, *General Lattice Theory*, Second edition, Birkhäuser Verlag, Basel, 1998

[7] G. Grätzer, *Universal Algebra*, Second edition, Springer, New York, 2008

[8] J. Hashimoto, *On Direct Product Decomposition of Partially Ordered Sets*, Ann. of Math. (2), Vol. 54, 1951, pp. 315–318

[9] R. D. Luce, *A Note on Boolean Matrix Theory*, Proc. Amer. Math. Soc., Vol. 3, No. 3, 1952, pp. 382–388

[10] G. Maze, C. Monico, J. Rosenthal, *Public Key Cryptography Based on Semigroup Actions*, Adv. Math. Commun., Vol. 1, No. 4, 2007, pp. 489–507

[11] C. Monico, *On Finite Congruence-Simple Semirings*, J. Algebra, Vol. 271, No. 2, 2004, pp. 846–854

[12] D. E. Rutherford, *Inverses of Boolean Matrices*, Proc. Glasgow Math. Assoc., Vol. 6, No. 1, 1963, pp. 49–53

[13] Y. Tan, *On Invertible Matrices Over Antirings*, Linear Algebra Appl., Vol. 423, 2007, pp. 428–444

[14] J. H. M. Wedderburn, *Boolean Linear Associative Algebra*, Ann. of Math., Vol. 35, No. 1, 1934, pp. 185–194

[15] C.-K. Zhao, *Inverses of L-Fuzzy Matrices*, Fuzzy Sets and Systems, Vol. 34, No. 1, 1990, pp. 103–116

[16] J. Zumbrägel, *Classification of Finite Congruence-Simple Semirings with Zero*, J. Algebra Appl., Vol. 7, No. 3, 2008, pp. 363–377